(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－7352
（P2002－7352A）
(43)公開日　平成14年1月11日(2002.1.11)

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
G06F 15/00	330	G06F 15/00	330F 5B085
H04L 9/32		H04L 9/00	673A 5J104
			673D

審査請求　未請求　請求項の数7　OL　（全 15 頁）

(21)出願番号　特願2000－191347(P2000－191347)

(22)出願日　平成12年6月26日(2000.6.26)

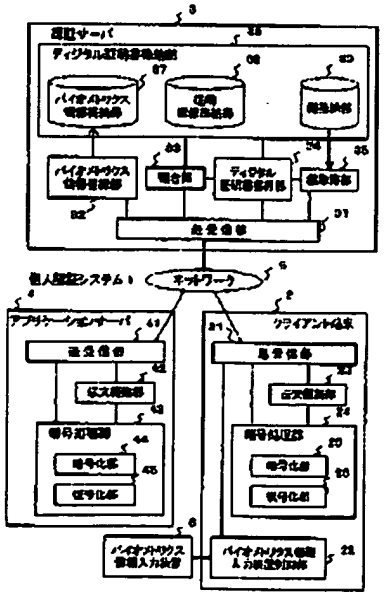
(71)出願人　000005234
富士電機株式会社
神奈川県川崎市川崎区田辺新田1番1号
(72)発明者　西田　廣治
神奈川県川崎市川崎区田辺新田1番1号
富士電機株式会社内
(74)代理人　100074099
弁理士　大菅　義之

Fターム(参考)　5B085 AE23 AE25 AE26 AE27 AE29
5j104 AA07 KA01 KA16 KA17 KA18
KA19 MA02 PA07

(54)【発明の名称】　個人認証システムおよび個人認証方法

(57)【要約】
【課題】　認証の安全性を高め、ディジタル証明書を認証サーバからダウンロードする場合もＩＤやパスワード等の入力無しに自動的に認証サーバからディジタル証明書をダウンロード可能にすることが課題である。
【解決手段】　アプリケーションサービスを提供するアプリケーションサーバとユーザが使用するクライアント端末とユーザを認証する認証サーバとが互いにネットワークを介して接続される個人認証システムにおける個人認証方法であって、クライアント端末を操作するユーザのバイオメトリクス情報を取得して認証サーバに送信し、予め認証サーバのディジタル証明書内に格納されたバイオメトリクス情報と照合してユーザが正規なユーザであるか否かを判断し、この判断により正規なユーザである場合は、伝文を暗号化して伝送する。

本発明の個人認証システムの構成ブロック図



1

【特許請求の範囲】

【請求項１】　アプリケーションサービスを提供するアプリケーションサーバとユーザが使用するクライアント端末と前記ユーザを認証する認証サーバとが互いにネットワークを介して接続される個人認証システムにおける個人認証方法であって、

前記クライアント端末が、前記クライアント端末を操作するユーザのバイオメトリクス情報を取得して前記認証サーバに送信し、

前記取得したバイオメトリクス情報を受信した前記認証サーバが、正規のユーザであることを示すディジタル証明書内に予め格納しているバイオメトリクス情報と照合することにより、前記ユーザが正規のユーザであるか否かを判断し、

前記判断により正規なユーザである場合は、前記認証サーバが、前記クライアント端末に対して前記ディジタル証明書を発行し、

前記ディジタル証明書を受信した前記クライアント端末が前記アプリケーションサーバのディジタル証明書を入手し、前記アプリケーションサーバに対して、前記クライアントのディジタル証明書によりディジタル署名を付し、前記アプリケーションサーバのディジタル証明書内の暗号化鍵により暗号化した伝文を伝送することを特徴とする個人認証方法。

【請求項２】　前記アプリケーションサーバが、前記ユーザ及び自アプリケーションサーバのディジタル証明書を取得し、受信した前記伝文を前記ユーザ及び前記アプリケーションサーバのディジタル証明書内の復号化鍵により復号化することを特徴とする請求項１に記載の個人認証方法。

【請求項３】　前記予め格納しているバイオメトリクス情報は、前記クライアント端末が、前記クライアント端末を操作するユーザのバイオメトリクス情報を取得して前記認証サーバに送信し、前記取得したバイオメトリクス情報を受信した前記認証サーバが、正規のユーザであることを示すディジタル証明書内に登録することを特徴とする請求項１または２に記載の個人認証方法。

【請求項４】　前記ディジタル証明書がバイオメトリクス認証に対応していない場合に、前記予め格納されたバイオメトリクス情報は、前記認証サーバが有する変換テーブルに、ユーザのＩＤ情報と対応させて格納されていることを特徴とする請求項１に記載の個人認証方法。

【請求項５】　前記バイオメトリクス情報は、指紋情報、虹彩情報、声紋情報、網膜パターン情報、筆跡情報またはＤＮＡ情報であることを特徴とする請求項１乃至４の何れか１項に記載の個人認証方法。

【請求項６】　アプリケーションサービスを提供するアプリケーションサーバとユーザが使用するクライアント端末とが互いにネットワークを介して接続される個人認証システムであって、

2

前記ネットワークに接続され、前記ユーザを認証する認証サーバを備え、

前記認証サーバは、

正規なアプリケーションサーバとしてあるいは正規なユーザとして登録してあることを証明する所定のディジタル証明書と、指紋情報、虹彩情報、声紋情報、網膜パターン情報、筆跡情報またはＤＮＡ情報であるバイオメトリクス情報を格納するバイオメトリクス情報格納部と、

前記ディジタル証明書に記されないディジタル証明項目の情報を格納する証明情報格納部と、暗号化鍵または復号化鍵を格納する鍵格納部とを有するディジタル証明書格納部と、

受信したバイオメトリクス情報と前記バイオメトリクス情報格納部に格納されたバイオメトリクス情報とを照合する照合部と、

前記ディジタル証明書を発行するディジタル証明書発行部と、

前記暗号化鍵または前記復号化鍵を取得する鍵取得部とを備え、

前記クライアント端末は、

前記バイオメトリクス情報を読み込むためのバイオメトリクス情報入力装置を制御するバイオメトリクス情報入力装置制御部と、

前記アプリケーションサーバへ伝送する伝文を編集する伝文編集部と、

前記伝文編集部が編集した伝文を暗号化し、前記アプリケーションサーバから伝送されてきた伝文を復号化する暗号化処理部とを備え、

前記アプリケーション端末は、

前記クライアント端末へ伝送する伝文を編集する伝文編集部と、

前記伝文編集部が編集した伝文を暗号化し、前記クライアント端末から伝送されてきた伝文を復号化する暗号化処理部とを備えることを特徴とする個人認証システム。

【請求項７】　前記認証サーバは、さらに、バイオメトリクス情報登録部を備えることを特徴とする請求項６に記載の個人認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、アプリケーションサーバとクライアント端末間の暗号文伝送に関し、特に、指紋、声紋等のバイオメトリクス情報によりクライアント端末を使用するユーザを認証する個人認証システムおよび個人認証方法に関する。

【０００２】

【従来の技術】現在、通信回線のインフラが整いつつあり、コンピュータをはじめとする情報機器は、通信回線を介して相互に接続されている。そして、我々ユーザは、情報機器を用い、通信回線を介して様々なサービスを利用することができるようになってきた。

【０００３】サービスの種類が増える一方で、金銭やプライバシーが絡むサービスにおいては、利用者が本人であることを確認することが必要である。また、自動的にパスワードを発見するプログラムを作成できる等、利用者に成りすまそうとする犯罪者にとっても好都合な環境が整いつつある。

【０００４】そこで、指紋、声紋等のバイオメトリクス情報を用いた照合は、管理や記憶の容易さや本人認証の正確さから、パスワード等に代わる方法として実現されている。

【０００５】従来は、アプリケーションサーバとクライアント端末間を公開鍵方式で暗号文伝送をするに当たり、アクセス権限を持ったユーザであるか否かの認証を指紋、虹彩、声紋、網膜パターン、筆跡、ＤＮＡなどのバイオメトリクス情報で認証を行う場合、ユーザが使用するクライアント端末内または、クライアント端末に接続されバイオメトリクス情報を入力するバイオメトリクス情報入力装置で照合をおこなっていた。

【０００６】さらに、認証サーバから証明書をダウンロードする際は、そのためのＩＤやパスワードを入力していた。また、特開平１１－１９５１２０号公報には、端末装置における電子文書の編集時に、カーソルが押印エリア（またはサインエリア）内に入ると、指紋検出部が編集者の指紋を検出し、その検出された指紋情報をホスト装置に送信する。そして、ホスト装置において、上記指紋情報が照合されることによりユーザ認証が行われ、同時に、照合された指紋情報と共に予め登録されている印章データ（またはサインデータ）が端末装置に返送される。端末装置では、その返送された印章データが押印エリアに書き込まれることにより、編集した電子文書に対する署名が実現される技術が開示されている。

【０００７】

【発明が解決しようとする課題】しかしながら、従来の個人認証システムまたは個人認証方法においては、バイオメトリクス情報で認証を行う場合、ユーザが使用するクライアント端末内または、クライアント端末に接続されバイオメトリクス情報を入力するバイオメトリクス情報入力装置で照合をおこなっていたため、照合の妥当性をアプリケーションサーバが確認できず、安全性の上で不十分であるという問題があった。

【０００８】本発明の課題は、認証の安全性を高め、ディジタル証明書を認証サーバからダウンロードする場合もＩＤやパスワード等の入力無しに自動的に認証サーバからディジタル証明書をダウンロード可能とする個人認証システムおよび個人認証方法を提供することである。

【０００９】

【課題を解決するための手段】本発明は、上記課題を解決するため、下記のような構成を採用した。すなわち、本発明の一態様によれば、本発明の個人認証方法は、アプリケーションサービスを提供するアプリケーションサーバとユーザが使用するクライアント端末と上記ユーザを認証する認証サーバとが互いにネットワークを介して接続される個人認証システムにおける個人認証方法であって、上記クライアント端末が、上記クライアント端末を操作するユーザのバイオメトリクス情報を取得して上記認証サーバに送信し、上記取得したバイオメトリクス情報を受信した前記認証サーバが、正規のユーザであることを示すディジタル証明書内に予め格納しているバイオメトリクス情報と照合することにより、上記ユーザが正規のユーザであるか否かを判断し、上記判断により正規なユーザである場合は、上記認証サーバが、上記クライアント端末に対して上記ディジタル証明書を発行し、上記ディジタル証明書を受信した上記クライアント端末が、上記アプリケーションサーバに対して、ディジタル証明書によりディジタル署名を付し、あらかじめ入手したアプリケーションサーバのディジタル証明書内の暗号化鍵により暗号化した伝文を伝送することを特徴とする。

【００１０】また、好適には、本発明の個人認証方法は、上記アプリケーションサーバが、上記ユーザのディジタル証明書を取得し、受信した上記ディジタル署名をディジタル証明書内の復号化鍵により復号化し、上記伝文を上記アプリケーションサーバのディジタル証明書内の復号化鍵により復号化する。

【００１１】また、好適には、本発明の個人認証方法は、上記予め格納しているバイオメトリクス情報が、上記クライアント端末によって、上記クライアント端末を操作するユーザのバイオメトリクス情報を取得されて上記認証サーバに送信され、上記取得したバイオメトリクス情報を受信した上記認証サーバによって、正規のユーザであることを示すディジタル証明書内に登録される。

【００１２】また、好適には、本発明の個人認証方法は、上記ディジタル証明書がバイオメトリクス認証に対応していない場合に、上記予め格納されたバイオメトリクス情報が、上記認証サーバが有する変換テーブルに、ユーザのＩＤ情報と対応させて格納されている。

【００１３】また、好適には、本発明の個人認証方法は、上記バイオメトリクス情報が、指紋情報、虹彩情報、声紋情報、網膜パターン情報、筆跡情報またはＤＮＡ情報である。

【００１４】また、本発明の一態様によれば、本発明の個人認証システムは、アプリケーションサービスを提供するアプリケーションサーバとユーザが使用するクライアント端末とが互いにネットワークを介して接続される個人認証システムであって、上記ネットワークに接続され、上記ユーザを認証する認証サーバを備え、上記認証サーバが、正規なアプリケーションサーバとしてあるいは正規なユーザとして登録してあることを証明する（例えば、Ｗｅｂブラウザがサポートするｓｓｌ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）プロトコル、電子商

取引用のＳＥＴ（Ｓｅｃｕｒｅ Ｅｌｅｃｔｒｏｎｉｃ Ｔｒａｎｓａｃｔｉｏｎｓ）プロトコル、電子メール用のＳ／ＭｉＭＥ（Ｓｅｃｕｒｅ ＭｕｌｔｉｐｕｒｐｏｓｅＩｎｔｅｒｎｅｔ Ｍａｉｌ Ｅｘｔｅｎｓｉｏｎｓ）などのように）ＩＴＵ－Ｔ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ Ｕｎｉｏｎ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ ｓｔａｎｄａｒｄｉｚａｔｉｏｎ：国際電気通信連合電気通信標準）により勧告されたＸ．５０９で定められたディジタル証明書と、指紋情報、虹彩情報、声紋情報、網膜パターン情報、掌跡情報またはＤＮＡ情報であるバイオメトリクス情報を格納するバイオメトリクス情報格納部と、前記ディジタル証明書に記されないディジタル証明項目の情報を格納する証明情報格納部と、暗号化鍵または復号化鍵を格納する鍵格納部とを有するディジタル証明書格納部と、受信したバイオメトリクス情報と上記バイオメトリクス情報格納部に格納されたバイオメトリクス情報とを照合する照合部と、上記ディジタル証明書を発行するディジタル証明書発行部と、上記暗号化鍵または上記復号化鍵を取得する鍵取得部とを備え、上記クライアント端末が、上記バイオメトリクス情報を読み込むためのバイオメトリクス情報入力装置を制御するバイオメトリクス情報入力装置制御部と、上記アプリケーションサーバへ伝送する伝文を編集する伝文編集部と、上記伝文編集部が編集した伝文を暗号化し、上記アプリケーションサーバから伝送されてきた伝文を復号化する暗号化処理部とを備え、上記アプリケーション端末が、上記クライアント端末へ伝送する伝文を編集する伝文編集部と、上記伝文編集部が編集した伝文を暗号化し、上記クライアント端末から伝送されてきた伝文を復号化する暗号化処理部とを備えることを特徴とする。

【００１５】また、好適には、本発明の個人認証システムは、上記認証サーバが、さらに、バイオメトリクス情報登録部を備える。

【００１６】

【発明の実施の形態】以下、本発明の実施の形態を、図面を参照しながら詳細に説明する。図１は、本発明の個人認証システムの機能ブロック図である。

【００１７】図１において、個人認証システム１は、アプリケーションサービスを提供するアプリケーションサーバ４と、ユーザが使用するクライアント端末２と、上記ユーザまたは上記アプリケーションサーバを認証する認証サーバ３とが互いにネットワーク５を介して接続され、クライアント端末２には、指紋、虹彩、声紋、網膜パターン、掌跡、ＤＮＡなどのバイオメトリクス情報を入力するためのバイオメトリクス情報入力装置６が接続されている。

【００１８】アプリケーションサーバ４は、ネットワーク５を介してクライアント端末２または認証サーバ３との間で、各種データ信号を送受信する送受信部４１と、クライアント端末２へ伝送する伝送文を編集する伝文編集部４２と、平文を暗号化する暗号化部４４と暗号文を元の平文に復号する復号化部４５とを有する暗号処理部４３とを備える。このアプリケーションサーバ４は、具体的には、プライベート情報を本人に通知するサービス等を行なう官公庁のホストコンピュータ、警報情報等を関係者に配信するための電力会社のホストコンピュータ、異常情報を関係者に配信するための浄水場の監視コンピュータ、または物流センター内の物流システムを構成するスタッカクレーン、無人搬送車、天井走行車、コンベア等の搬送機器や、各種センサ、制御装置、通信装置等の多種多様な機器の予防保全データを各リモートメンテナンス企業へ送付する物流センターのホストコンピュータ等である。

【００１９】クライアント端末２は、ネットワーク５を介してアプリケーションサーバ４または認証サーバ３との間で、各種データ信号を送受信する送受信部２１と、アプリケーションサーバ４へ伝送する伝送文を編集する伝文編集部２３と、平文を暗号化する暗号化部２５と暗号文を元の平文に復号する復号化部２６とを有する暗号処理部２４と、バイオメトリクス情報入力装置６がバイオメトリクス情報を読み取るように制御し、バイオメトリクス情報入力装置６が読み取ったバイオメトリクス情報を認証サーバに送信するよう制御するバイオメトリクス情報入力装置制御部２２とを備える。

【００２０】認証サーバ３は、ネットワーク５を介してクライアント端末２またはアプリケーションサーバ４との間で、各種データ信号を送受信する送受信部３１と、ディジタル証明書を格納するディジタル証明書格納部３６と、ディジタル証明書格納部３６の所定の領域にバイオメトリクス情報を格納させるバイオメトリクス情報登録部３２と、クライアント端末２から送信されてきたバイオメトリクス情報がバイオメトリクス情報格納部３７に予め格納されたバイオメトリクス情報と合致するか否かを照合する照合部３３と、予めディジタル証明書格納部３６に格納され、正規なアプリケーションサーバとしてあるいは正規なユーザとして登録してあることを証明するディジタル証明書を発行するディジタル証明書発行部３４と、ディジタル証明書格納部３６の所定の領域に格納された暗号化鍵または復号化鍵を取得する鍵取得部３５とを備える。

【００２１】また、ディジタル証明書格納部３６は、所定の領域に、バイオメトリクス情報を格納するバイオメトリクス情報格納部３７と、氏名や電子メールアドレスなどＸ．５０９（ＩＴＵ－Ｔ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ Ｕｎｉｏｎ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ ｓｔａｎｄａｒｄｉｚａｔｉｏｎ：国際電気通信連合電気通信標準）により勧告されたＸ．５０９）で定められた必須項目を格納する証明情報格納部３８及び、暗号鍵を格納す

る鍵格納部３９とを有する。

【００２２】図２および図３は、本発明における暗号文伝送時のプログラム処理フローを示す図である。図２において、送信処理が開始されると、ステップＳ２１で、クライアント端末またはアプリケーションサーバが有する伝送アプリケーションは、伝送する伝文を編集し、ステップＳ２２で、暗号ミドルウェア関数を呼び出す。図３に移り、暗号ミドルウェア関数は、ステップＳ３１で、パラメータで渡された伝送プロトコル種別を判定し、ステップＳ３２で、伝送プロトコルに対応した公開鍵暗号方式の暗号ツールを選択する。その後、ステップＳ３３で、ディジタル証明書から暗号化鍵（送信元である自分（例えば、クライアント端末またはアプリケーションサーバ）の秘密鍵と送信先である相手（送信元がクライアント端末の場合はアプリケーションサーバ、送信元がアプリケーションサーバの場合はクライアント端末）の公開鍵）を取得し、暗号化処理を行う。そして、ステップＳ３４で、その暗号化された伝文を送受信部で伝送処理（送受信）する。

【００２３】伝文を受信する場合は、送受信部が伝文を取り出し、暗号ミドルウェアを呼び出す。ユーザ本人が認証されていない場合は、認証した時点で暗号ミドルウェアを呼び出す。暗号ミドルウェアではパラメータで渡された伝送プロトコル種別を判定し、伝送プロトコルに対応した公開鍵暗号方式の暗号ツールを選択する。その後、ディジタル証明書から復号化鍵を取得し、復号化処理を行う。その復号化された伝文を受信伝文とする。

【００２４】図４は、本発明におけるバイオメトリクス情報を登録する処理を説明するためのフローチャートである。図４において、バイオメトリクス情報を登録する処理が開始されると、ステップＳ４１で、バイオメトリクス情報入力装置は、ユーザのバイオメトリクス情報、例えば指紋情報を読み取る。そして、ステップＳ４２で、読み取った指紋情報等の特徴点情報を抽出等して、バイオメトリクス情報入力装置に接続されたクライアント端末へ上記バイオメトリクス情報を送信する。

【００２５】ステップＳ４３で、バイオメトリクス情報入力装置から送信されたバイオメトリクス情報を受信したクライアント端末は、ネットワークを介して認証サーバへ上記バイオメトリクス情報を送信（転送）する。

【００２６】ステップＳ４４で、認証サーバは、クライアント端末から送信されたバイオメトリクス情報を受信する。ステップＳ４５で、バイオメトリクス情報を受信した認証サーバは、バイオメトリクス情報登録部によりディジタル証明書格納部の所定領域に設けられたバイオメトリクス情報格納部に上記バイオメトリクス情報を格納する。

【００２７】このようにして、クライアント端末を利用する各ユーザのバイオメトリクス情報は、クライアント端末およびアプリケーションサーバにネットワークを介して接続された認証サーバのディジタル証明書格納部にあらかじめ登録される。

【００２８】図５および図６は、本発明におけるクライアント端末からアプリケーションサーバへ暗号文を伝送する処理を説明するためのフローチャートである。図５において、クライアント端末からアプリケーションサーバへ暗号文を伝送する前処理として、ステップＳ５１で、バイオメトリクス情報入力装置は、上記暗号文を伝送しようとするユーザのバイオメトリクス情報、例えば指紋情報を読み取る。そして、ステップＳ５２で、読み取った指紋情報の特徴点情報を抽出等して、バイオメトリクス情報入力装置に接続されたクライアント端末へ上記バイオメトリクス情報を送信する。

【００２９】ステップＳ５３で、バイオメトリクス情報入力装置から送信されたバイオメトリクス情報を受信したクライアント端末は、ネットワークを介して認証サーバへ上記バイオメトリクス情報を送信（転送）する。

【００３０】ステップＳ５４で、認証サーバは、クライアント端末から送信されたバイオメトリクス情報を受信する。ステップＳ５５で、バイオメトリクス情報を受信した認証サーバは、受信したバイオメトリクス情報がバイオメトリクス情報格納部に格納されているか否か、すなわち、正規なユーザとして登録されているか否かを照合部によって照合する。

【００３１】そして、上記照合の結果、ステップＳ５６で、認証サーバの受信したバイオメトリクス情報とバイオメトリクス情報格納部に格納されているバイオメトリクス情報とが合致するか否かを判断する。合致した場合（ステップＳ５６：ＹＥＳ）は、ステップＳ５７で、ディジタル証明書発行部により上記暗号文を伝送しようとするユーザが正規なユーザとして登録されている旨のディジタル証明書を、ディジタル署名のための暗号化鍵（例えば、秘密鍵）と共に、正規なユーザとして登録されているか否かを問い合わせてきたクライアント端末に対して発行（送信）する。なお、上記暗号化鍵は、鍵取得部が鍵格納部から取得し、ディジタル証明書発行部に渡す。

【００３２】正規なユーザとして登録されているか否かを問い合わせたクライアント端末は、ステップＳ５８で、上記ディジタル証明書を受信する（前処理終了）。続いて、伝送処理の説明に移る。ステップＳ５９で、ディジタル証明書と共に受信した暗号化鍵で、アプリケーションサーバに伝送したい伝文に対してディジタル署名をする。そして、図６に移り、ステップＳ６０で、上記ディジタル署名をした伝文（平文）自体をあらかじめ入手したアプリケーションサーバの暗号化鍵（例えば、公開鍵）で暗号化する。ステップＳ６１で、暗号化した暗号文を伝送先のアプリケーションサーバに対して送信する。

【００３３】アプリケーションサーバは、ステップＳ６

２で．上記暗号文を受信し．ステップＳ６３で．あらかじめ認証サーバから入手したユーザの復号化鍵（例えば．公開鍵）で受信した暗号文のディジタル署名を復号化する。

【００３４】ステップＳ６４で、暗号文のディジタル署名を復号化したアプリケーションサーバは、上記復号化が正常に行なわれたか否か．すなわち．ディジタル署名を行なった暗号化鍵のユーザの復号化鍵で復号化したか否かを判断する。

【００３５】そして、上記判断により．正規のユーザからの伝文伝送であるとされた場合（ステップＳ６４：ＹＥＳ）は、ステップＳ６５で、暗号化された伝文自体をあらかじめ入手した復号化鍵（例えば．秘密鍵であり、この復号化鍵は．アプリケーションサーバのディジタル証明書（正規なアプリケーションサーバとして登録されている旨のディジタル証明書）とともに入手可能）で復号化する。なお．正常に復号化されず．正規のユーザからの伝送伝文でないとされた場合（ステップＳ６４：ＮＯ）は、例えば．上記伝文を破棄し．クライアント端末に対して異常応答をして終了する。

【００３６】図７および図８は、本発明におけるアプリケーションサーバからクライアント端末へ暗号文を伝送する処理を説明するためのフローチャートである。図７において、アプリケーションサーバからクライアント端末へ暗号文を伝送する処理が開始されると、前処理としてディジタル証明書を入手する。すなわち、アプリケーションサーバからの伝送先とされたクライアント端末が．ステップＳ７１で、バイオメトリクス情報入力装置に対して、クライアント端末を操作しているユーザのバイオメトリクス情報を入力するように要求する。

【００３７】ステップＳ７２で、バイオメトリクス情報を入力するように要求されたバイオメトリクス情報入力装置は、上記ユーザのバイオメトリクス情報、例えば指紋情報を読み取る。そして．ステップＳ７３で．読み取った指紋情報の特徴点情報を抽出等して、バイオメトリクス情報入力装置に接続されたクライアント端末へ上記バイオメトリクス情報を送信する。

【００３８】ステップＳ７４で、バイオメトリクス情報入力装置から送信されたバイオメトリクス情報を受信したクライアント端末は、ネットワークを介して認証サーバへ上記バイオメトリクス情報を送信（転送）する。

【００３９】ステップＳ７５で、認証サーバは．クライアント端末から送信されたバイオメトリクス情報を受信する。ステップＳ７６で．バイオメトリクス情報を受信した認証サーバは、受信したバイオメトリクス情報がバイオメトリクス情報格納部に格納されているか否か、すなわち、正規なユーザとして登録されているか否かを照合部によって照合する。

【００４０】そして、上記照合の結果．ステップＳ７７で．認証サーバの受信したバイオメトリクス情報とバイオメトリクス情報格納部に格納されているバイオメトリクス情報とが合致するか否かを判断する。合致した場合（ステップＳ７７：ＹＥＳ）は、ステップＳ７８で、ディジタル証明書発行部により上記暗号文を復号化しようとするユーザが正規なユーザとして登録されている旨のディジタル証明書を、暗号文を復号化するための復号化鍵（例えば、公開鍵）と共に、正規なユーザとして登録されているか否かを問い合わせてきたクライアント端末に対して発行（送信）する。なお、上記暗号化鍵は、鍵取得部が鍵格納部から取得し、ディジタル証明書発行部に渡す。

【００４１】正規なユーザとして登録されているか否かを問い合わせたクライアント端末は．ステップＳ７９で．上記ディジタル証明書を受信する（前処理終了）。続いて、図８を用いて伝送処理について説明する。ステップＳ８０で．あらかじめ入手したディジタル証明書と共に受信した暗号化鍵（例えば、秘密鍵）で、クライアント端末に伝送したい伝文に対してディジタル署名をする。さらに、ステップＳ８１で、上記ディジタル署名をした伝文（平文）自体をクライアント端末の暗号化鍵（例えば、公開鍵）で暗号化する。そして、ステップＳ８２で、暗号化した暗号文を伝送先のクライアント端末に対して送信する。

【００４２】クライアント端末は、ステップＳ８３で、上記暗号文を受信し、ステップＳ８４で、あらかじめ認証サーバから入手したアプリケーションサーバの復号化鍵（例えば、公開鍵）で受信した暗号文のディジタル署名を復号化する。

【００４３】ステップＳ８５で、暗号文のディジタル署名を復号化したクライアント端末は．上記復号化が正常に行なわれたか否か、すなわち、ディジタル署名を行なった暗号化鍵のアプリケーションサーバの復号化鍵で復号化したか否かを判断する。

【００４４】そして、上記判断により．正規のアプリケーションサーバからの伝文伝送であるとされた場合（ステップＳ８５：ＹＥＳ）は．ステップＳ８６で．暗号化された伝文自体をあらかじめ入手した復号化鍵（例えば．秘密鍵であり、この復号化鍵は．アプリケーションサーバのディジタル証明書（正規なアプリケーションサーバとして登録されている旨のディジタル証明書）とともに入手可能）で復号化する。

【００４５】なお、上述してきたようなバイオメトリクス情報は、ディジタル証明書の運用方法に対応して、必要に応じ、変換テーブルにＩＤとバイオメトリクス情報との対を持つことにより．ディジタル証明書の外部に持つことも可能である。

【００４６】また、ディジタル証明書内にバイオメトリクス情報を有する場合は．ユーザがクライアント端末で認証する時点において、ディジタル証明書を取得済でありディジタル証明書の有効期限内である時は、クライア

ント端末で入力されるバイオメトリクス情報とディジタル証明書のバイオメトリクス情報を照合することも可能である。

【００４７】上述してきたような、アプリケーションサービスを提供するアプリケーションサーバと、ユーザが使用するクライアント端末と、ユーザを認証する認証サーバとが互いにネットワークを介して接続される個人認証システムは、以下のような形態に特に有効である。

【００４８】（１）官公庁における、イントラネットまたはインターネットを介したプライバシー情報などの本人への送付。

（２）電力会社での電力の系統制御における、イントラネットまたはインターネットを介した警報情報の関係者への配信。

【００４９】（３）浄水場の監視制御における、イントラネットまたはインターネットを介した異常情報の関係者への配信。

（４）物流センターや工場における、イントラネットまたはインターネットを介した予防保全データのリモートメンテナンス企業への送付。

【００５０】上述のように、本発明の実施の形態を、図面を参照しながら説明してきたが、説明したクライアント端末、認証サーバ、およびアプリケーションサーバは、汎用の情報処理装置（コンピュータ）を用いて構成することができる。上記情報処理装置は、ＣＰＵ（中央処理装置）、メモリ、入力装置、出力装置、外部記憶装置、媒体駆動装置、およびネットワーク接続装置を備え、これらはバスにより互いに接続されている。

【００５１】メモリは、例えば、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）等を含み、処理に用いられるプログラムとデータを格納する。ＣＰＵは、メモリを利用してプログラムを実行することにより、必要な処理を行う。

【００５２】入力装置は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、ユーザからの指示や情報の入力に用いられる。出力装置は、例えば、ディスプレイ、プリンタ、スピーカ等であり、ユーザへの問い合わせや処理結果の出力に用いられる。

【００５３】外部記憶装置は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。情報処理装置は、この外部記憶装置に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリにロードして使用することができる。また、外部記憶装置は、登録データ、登録データの種類、ＩＤ番号等を保存するデータベースとしても用いることができる。

【００５４】媒体駆動装置は、可搬記録媒体を駆動し、その記録内容にアクセスする。可搬記録媒体としては、メモリカード、フロッピーディスク、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｋ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。管理者は、この可搬記録媒体に上述のプログラムとデータを格納しておき、情報処理装置は、必要に応じて、それらをメモリにロードして使用することができる。

【００５５】ネットワーク接続装置は、任意のネットワーク（回線）を介して外部の装置と通信し、通信に伴うデータ変換を行う。また、情報処理装置は、必要に応じて、ネットワーク接続装置を介して上述のプログラムとデータを外部の装置から受け取り、それらをメモリにロードして使用することができる。

【００５６】すなわち、本発明は、以上に述べた実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲内で種々の構成または形状を取ることが出来る。

【００５７】

【発明の効果】本発明によれば、アプリケーションサーバとクライアント端末との間で暗号文を伝送する場合に、認証サーバが格納しているディジタル証明書で照合を行うため、伝文伝送の安全性を高める事ができる。

【００５８】また、本発明によれば、ディジタル証明書を認証サーバからダウンロードする場合も、従来必要とされていたＩＤやパスワード等を入力を行なわずに、バイオメトリクス情報を用いた認証により自動で認証サーバからディジタル証明書をダウンロードすることを可能となる。

【００５９】また、本発明によれば、ユーザのＩＤ情報の変換テーブルを有することにより、バイオメトリクス情報を有しないディジタル証明書であっても同様の処理が可能となる。

【００６０】すなわち、本発明によれば、アプリケーションサーバとクライアント端末との間のネットワークの情報は、暗号化され、クライアント端末における認証によりアクセス権限が確認される。これにより、盗聴、改ざん、なりすましを防止することができ、インターネットやイントラネットに接続した任意のクライアント端末からいつでも高い安全性でアプリケーションサーバの情報を取得できる。さらに、取得もユーザから要求するだけでなく、アプリケーションサーバから随時送付できる。

【００６１】また、本発明のよれば、バイオメトリクス情報を用いた認証により、ＩＤやパスワード等の入力のわずらわしさを回避することができる。

【図面の簡単な説明】

【図１】本発明の個人認証システムの機能ブロック図である。

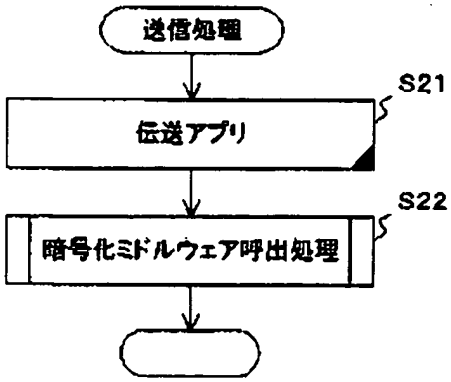
【図２】本発明における暗号文伝送時のプログラム処理フローを示す図（その１）である。

【図３】本発明における暗号文伝送時のプログラム処理フローを示す図（その２）である。

【図４】本発明におけるバイオメトリクス情報を登録する処理を説明するためのフローチャートである。
【図５】本発明におけるクライアント端末からアプリケーションサーバへ暗号文を伝送する処理を説明するためのフローチャート（その１）である。
【図６】本発明におけるクライアント端末からアプリケーションサーバへ暗号文を伝送する処理を説明するためのフローチャート（その２）である。
【図７】本発明におけるアプリケーションサーバからクライアント端末へ暗号文を伝送する処理を説明するためのフローチャート（その１）である。
【図８】本発明におけるアプリケーションサーバからクライアント端末へ暗号文を伝送する処理を説明するためのフローチャート（その２）である。
【符号の説明】
１　個人認証システム
２　クライアント端末
３　認証サーバ
４　アプリケーションサーバ４
５　ネットワーク
６　バイオメトリクス情報入力装置
＊２１　送受信部
２２　バイオメトリクス情報入力装置制御部
２３　伝文編集部
２４　暗号処理部
２５　暗号化部
２６　復号化部
３１　送受信部
３２　バイオメトリクス情報登録部
３３　照合部
３４　ディジタル証明書発行部
３５　鍵取得部
３６　ディジタル証明書格納部
３７　バイオメトリクス情報格納部
３８　証明情報格納部
３９　鍵格納部
４１　送受信部
４２　伝文編集部
４３　暗号処理部
４４　暗号化部
４５　復号化部

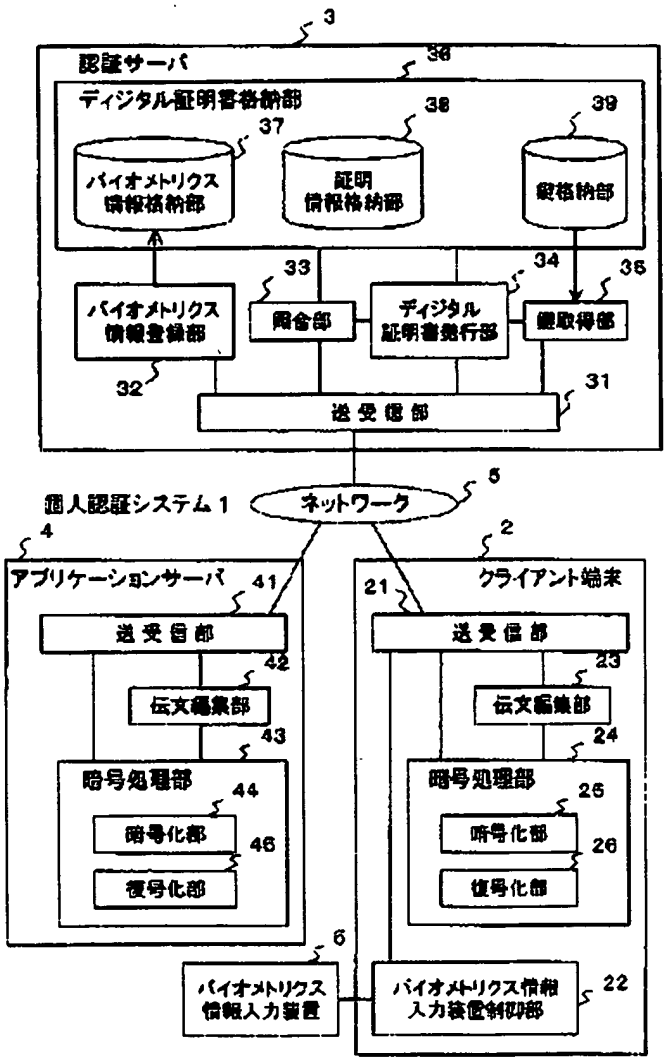
【図２】

本発明における暗号文伝送時の
プログラム処理フローを示す図(その1)



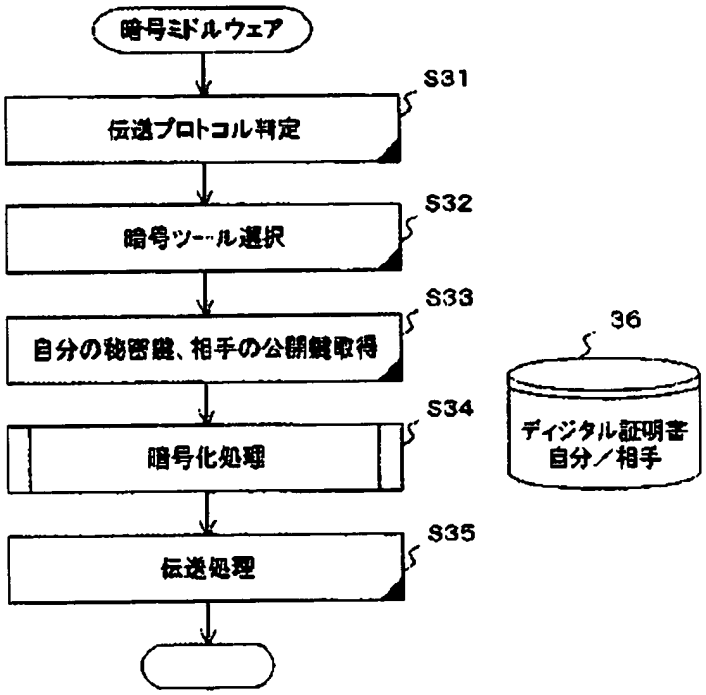
【図1】

本発明の個人認証システムの機能ブロック図



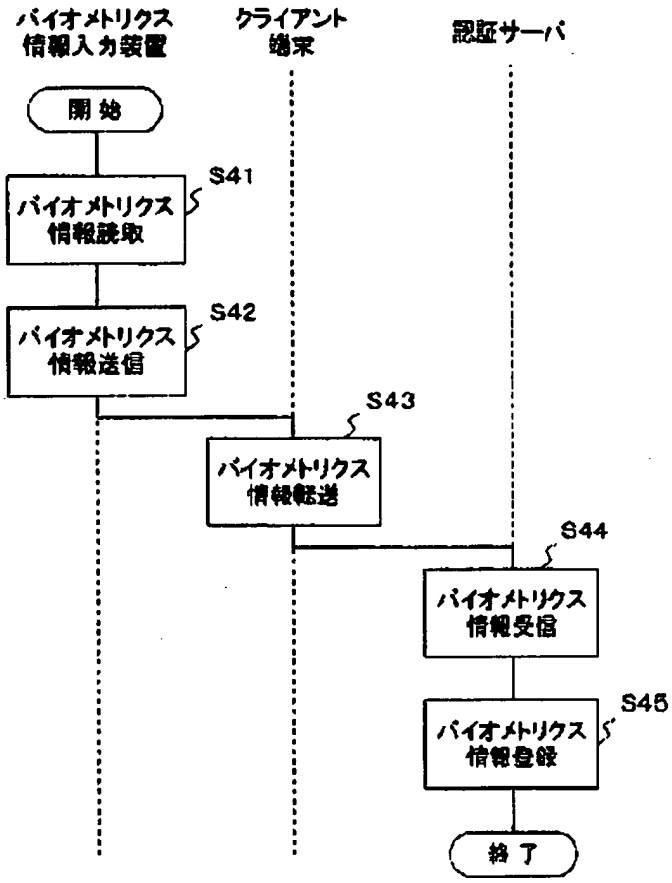
【図３】

本発明における暗号文伝送時の
プログラム処理フローを示す図(その2)



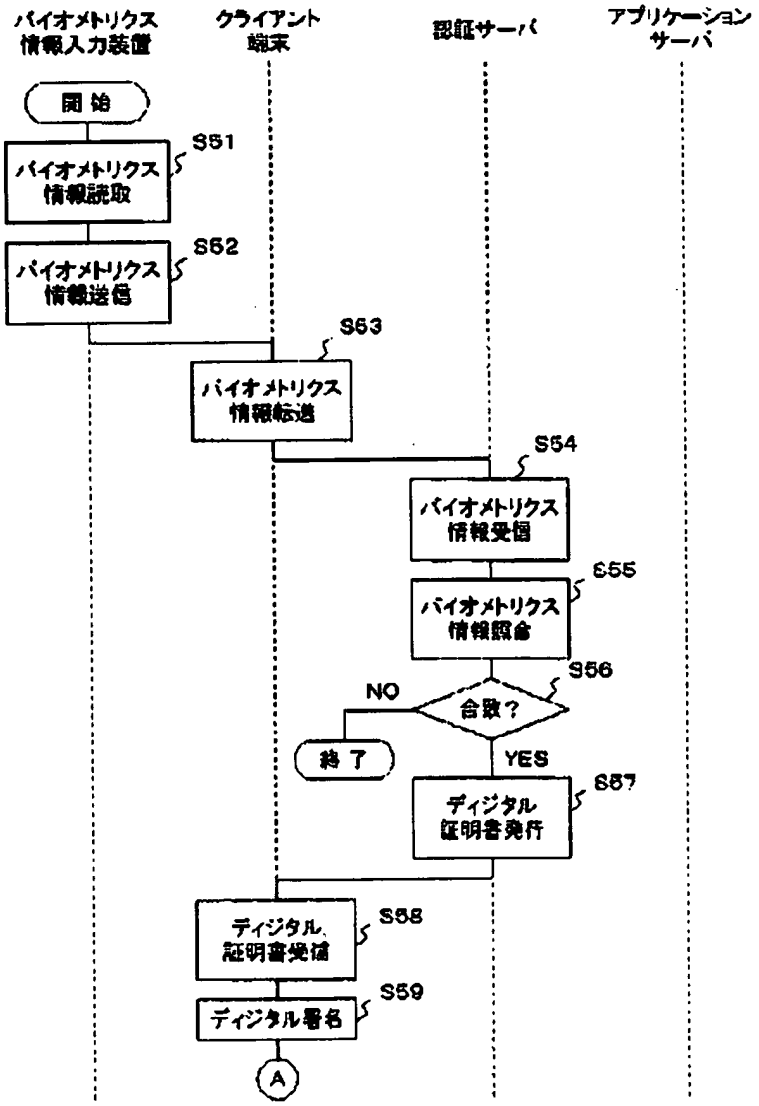
【図4】

本発明におけるバイオメトリクス情報を
登録する処理を説明するためのフローチャート



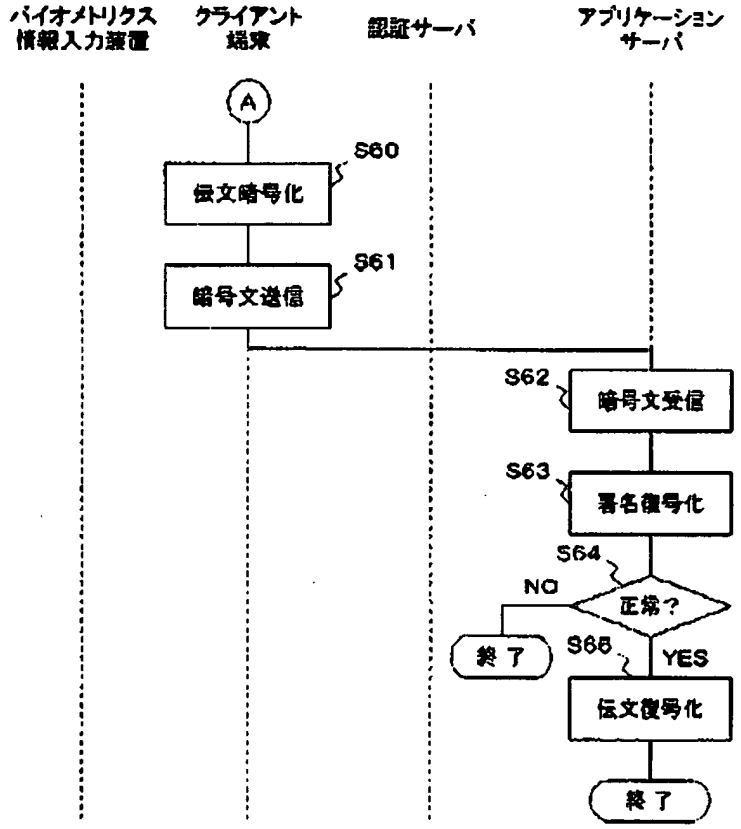
【図5】

本発明におけるクライアント端末からアプリケーションサーバへ
暗号文を伝送する処理を説明するためのフローチャート(その1)



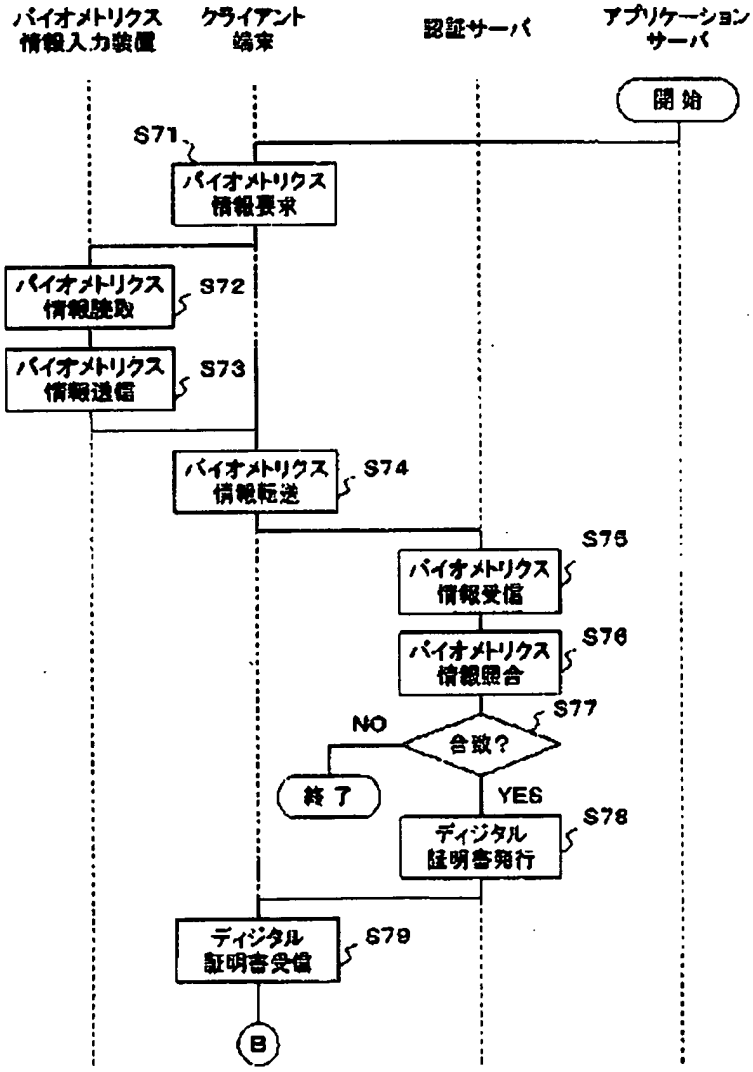
【図6】

本発明におけるクライアント端末からアプリケーションサーバへ
暗号文を伝送する処理を説明するためのフローチャート(その2)



【図７】

本発明におけるアプリケーションサーバからクライアント端末へ
暗号文を伝送する処理を説明するためのフローチャート(その１)



【図８】

本発明におけるアプリケーションサーバからクライアント端末へ
暗号文を伝送する処理を説明するためのフローチャート（その２）